

SECTIONS ON CERTAIN  $j = 0$  ELLIPTIC SURFACES

JASBIR CHAHAL, MATTHIJS MEIJER, AND JAAP TOP

## 1. INTRODUCTION

It is well known that elliptic curves  $E$  over a function field  $k(t)$  are in 1-1 correspondence with elliptic surfaces  $\mathcal{E} \rightarrow \mathbb{P}^1$  over  $k$ . The geometric interpretation of points in  $E(k(t))$  arising in this way has led to a lot of results; see, e.g., [Sh72], [Sh90]. For instance, if  $\text{char}(k) = 0$  and  $E$  is not isomorphic over  $k(t)$  to a curve already defined over  $k$ , then  $\text{rank } E(k(t)) \leq 10p_g + 8$ , where  $p_g$  is the geometric genus (the number of independent regular 2-forms) of the elliptic surface.

In case the surface is rational one has  $p_g = 0$  and hence the upper bound above equals 8. The pencil of cubic curves passing through 8 given points (in general position) in the plane provides an example of such a surface. The 9 base points of the pencil yield sections of the surface, and with any one of them as origin the others are (in the general case) independent. More details on this are found in [Sh90] and references given there. In fact it is not hard to construct rational surfaces with any rank between 0 and 8. In particular explicit examples exist even with a basis for the group  $E(k(t))$ .

It is interesting to note that the upper bound  $10p_g + 8$  is not known to be sharp for high geometric genus. In fact it is not even known whether  $\text{rank } E(\mathbb{C}(t))$  can attain arbitrarily high values. The current record seems to be due to Shioda (1992). He asserts in [Sh92] that the curve given by  $y^2 = x^3 + t^{360} + 1$  has rank 68 over  $\mathbb{C}(t)$ . This example has  $p_g = 59$  hence the actual rank is much smaller than the general theoretical upper bound. We will discuss this example in more detail below (proposition 4.2).

The smallest case beyond rational surfaces is the one with  $p_g = 1$ , so ranks  $\leq 10 \cdot 1 + 8 = 18$ . The elliptic surfaces in this case are so-called  $K3$ -surfaces. A result of David Cox states that any integer  $r$  with  $0 \leq r \leq 18$  occurs as the rank of some elliptic  $K3$ -surface over  $\mathbb{C}$ ; see [Co] and also [Ni]. The proof uses the surjectivity of a period map, and is therefore transcendental in nature. In particular, it does not give equations of such surfaces, let alone explicit descriptions of independent sections. A different proof for the existence of elliptic  $K3$ -surfaces with Mordell-Weil rank 18 is presented in Kuwata's paper [Ku]. It is based on work of Inose which implies, that

---

*Date:* November 1999.

This work originated from a lecture by Masato Kuwata during the 914th AMS meeting at Rider university, Lawrenceville, New Jersey in October 1996. The third author would like to thank Henri Darmon and Fernando Rodriguez Villegas for inviting him to this meeting, and Masato Kuwata and Jasper Scholten for their interest in this work. Several ideas in this paper were developed during the summer of 1998 which the third author spent at BYU. He thanks Jasbir Chahal, Bill Lang and Tyler Jarvis for their hospitality. The middle section of this paper was a part of the second author's Master's thesis in mathematics at the university of Groningen.

if a rational map of finite degree exists between  $K3$ -surfaces, then they have the same Néron-Severi rank ([In, Cor. 1.2]). Kuwata starts with the Kummer surface of a product  $E_1 \times E_2$  of isogenous CM-elliptic curves. He then constructs a degree 3 cover of it which is still  $K3$ , and which moreover in many cases admits an elliptic fibration without reducible fibres. This easily implies that the resulting example has Mordell-Weil rank 18. It is straightforward to write down explicit examples of such surfaces, even with equations over  $\mathbb{Q}$  (although the sections will usually only be defined over an extension). However, from the transcendental nature of the result of Inose, it remains unclear how to find independent sections for these examples.

In the present paper we present an example with an explicit description of 18 independent sections:

**Theorem 1.1.** *The elliptic curve  $E/\mathbb{Q}(t)$ , defined by the equation  $y^2 = x^3 - 27(t^{12} - 11t^6 - 1)$  corresponds to a  $K3$ -surface. It has rank  $E(\overline{\mathbb{Q}}(t)) = 18$ .*

*One finds 18 independent points among the  $(x(t), y(t)) \in E(\overline{\mathbb{Q}}(t))$  where  $x(t)$  has one of the forms*

$$\frac{at^{12} + bt^6 + c}{t^n}$$

or

$$\frac{\omega(t^{24} - 12t^{18} + 14t^{12} + 12t^6 + 1)}{4t^{10}},$$

with  $n \in \{0, 2, 4, 6, 8\}$  and  $\omega^3 = 1$ .

It seems plausible that one can prove this by merely finding sufficiently many points as in the theorem, and then calculating a height pairing determinant. However, we have not tried this rather uninteresting and elaborate method. Instead, we give a proof which is hopefully more enlightening. It relies on the fact that the elliptic curve given in the theorem has  $j$ -invariant 0. Some Galois theory and linear algebra then allow one to break the Mordell-Weil group into parts. Most of these parts correspond to Mordell-Weil groups of rational elliptic surfaces, which are well understood.

We finish the paper by applying the same method to the problem of constructing high rank curves over function fields. In particular, the rank 68 example of Shioda is studied, and we mention some examples of elliptic curves of a similar form with a fairly high  $\mathbb{Q}(t)$ -rank.

## 2. GENERALITIES ON $j = 0$ ELLIPTIC CURVES

Suppose  $E$  is an elliptic curve defined over a field  $K$ . For any finite extension  $L/K$ , the Galois group  $\text{Gal}(L/K)$  acts on the group  $E(L)$  of  $L$ -rational points of  $E$ . Regarding  $E(L)$  as a module over  $R := \text{End}_K(E)$ , this Galois action is  $R$ -linear. This can be used to decompose  $E(L)$ , or rather the vector space  $E(L) \otimes_{\mathbb{Z}} \mathbb{Q}$ , as a direct sum of smaller vector spaces.

The standard example where this is used, is given by a quadratic Galois extension  $L/K$ . The Galois action splits  $E(L) \otimes_{\mathbb{Z}} \mathbb{Q}$  as  $V^+ \oplus V^-$ . Here  $V^+$  consists of the elements in  $E(L) \otimes_{\mathbb{Z}} \mathbb{Q}$  on which  $\text{Gal}(L/K)$  acts trivially; hence  $V^+ = E(K) \otimes_{\mathbb{Z}} \mathbb{Q}$ . The other space  $V^-$  consists of the points in  $E(L) \otimes_{\mathbb{Z}} \mathbb{Q}$  on which  $\text{Gal}(L/K)$  acts via the non-trivial character of order 2. In other words, if  $\tau \in \text{Gal}(L/K)$  is the generator, then  $V^-$  consists of all  $P \otimes r$  for which  $\tau(P) = -P$ . This implies that  $V^-$  can be identified with

$E'(K) \otimes_{\mathbb{Z}} \mathbb{Q}$ , in which  $E'$  is the quadratic twist of  $E/K$  over  $L$ . In particular, if we are in a situation where the Mordell-Weil theorem holds, then

$$\text{rank } E(L) = \text{rank } E(K) + \text{rank } E'(K)$$

(compare [Sil, exerc. X-10.16]) as is well known.

We will use such a splitting in the case that  $\text{End}_K(E)$  has field of fractions  $\mathbb{Q}(\omega)$ , for a primitive cube root of unity  $\omega$ . Suppose that we are in this case. Then for any extension  $L/K$ , the vector space  $E(L) \otimes_{\mathbb{Z}} \mathbb{Q}$  is a linear space over  $\mathbb{Q}(\omega)$ . In particular, if  $L/K$  is a Galois extension with a cyclic Galois group  $\langle \sigma \rangle$  of order 6, then  $\sigma$  acts  $\mathbb{Q}(\omega)$ -linearly on  $E(L) \otimes_{\mathbb{Z}} \mathbb{Q}$ . Since all eigenvalues  $\lambda$  of  $\sigma$  satisfy  $\lambda^6 = 1$ , they are  $\mathbb{Q}(\omega)$ -rational, hence  $E(L) \otimes_{\mathbb{Z}} \mathbb{Q}$  splits as a direct sum  $\sum V_{\lambda}$ . Here  $V_{\lambda}$  is the  $\mathbb{Q}(\omega)$ -vector space consisting of the points  $P \otimes r \in E(L) \otimes_{\mathbb{Z}} \mathbb{Q}$  for which  $\tau(P) = \lambda P$ . As in the standard example, each  $V_{\lambda}$  can be interpreted in terms of  $K$ -rational points on a certain (quadratic or cubic or sextic) twist of  $E/K$  over  $L$ .

This is made explicit in the following example.

**Lemma 2.1.** *Let  $k/\mathbb{Q}(\omega)$  be a field extension and let  $K = k(s)$  be a purely transcendental extension of  $k$ . Consider  $L := k(t)$  over  $K$ , in which  $t^6 = s$ . Then  $L/K$  is cyclic of degree 6.*

*If  $E/K$  is the elliptic curve defined by the equation  $y^2 = x^3 + f(s)$  for some rational function  $f(s) \in K$ , then the  $\mathbb{Q}(\omega)$ -vector space  $E(L) \otimes_{\mathbb{Z}} \mathbb{Q}$  splits as a direct sum*

$$\sum_{n=0}^5 V_{(-\omega^2)^n}.$$

*The  $\mathbb{Q}(\omega)$ -vector space  $V_{(-\omega^2)^n}$  here can be identified with  $E_n(K) \otimes_{\mathbb{Z}} \mathbb{Q}$ , in which  $E_n/K$  is the elliptic curve given by  $y^2 = x^3 + s^n f(s)$ .*

*Proof.* Fix  $\text{End}_K(E) \cong \mathbb{Z}[\omega]$  by identifying  $\omega$  with the endomorphism  $(x, y) \mapsto (\omega x, y)$ . The only statement of the lemma which is not explained in the discussion above, is the identification of the eigenspace  $V_{(-\omega^2)^n}$  with  $E_n(K) \otimes_{\mathbb{Z}} \mathbb{Q}$ . This is a direct consequence of the fact that  $P = (x(t), y(t))$  is in  $E(L)$  and satisfies  $(x(-\omega^2 t), y(-\omega^2 t)) = (-\omega^2)^n P$ , precisely when  $(t^{2n} x(t), t^{3n} y(t)) \in E_n(K)$ . This shows in particular how a point  $P \otimes r \in V_{(-\omega^2)^n}$  yields an element of  $E_n(K)$ . Conversely,  $(x(s), y(s)) \in E_n(K)$  is sent to  $(x(t^6)/t^{2n}, y(t^6)/t^{3n}) \in E(L)$  in the associated eigenspace.  $\square$

In the rest of this paper we only consider  $j = 0$  elliptic curves  $E/K$ , given by an equation  $y^2 = x^3 + k$ . Note that for  $\omega \in K$  the  $\mathbb{Z}[\omega]$ -module structure on  $E(K)$  implies, that if  $P \in E(K)$  is a point of infinite order, then so is  $\omega P$ , and  $P, \omega P \in E(K)$  are independent (over  $\mathbb{Z}$ ). More generally, the fact that the  $\mathbb{Z}$ -module  $E(K)$  is even a  $\mathbb{Z}[\omega]$ -module, shows that if it has finite rank over  $\mathbb{Z}$ , then this rank is even. Some related information is given in the following lemma.

**Lemma 2.2.** *Suppose that  $\text{rank } E(K)$  is finite, and that  $L := K(\sqrt{-3})$  is a quadratic extension of  $K$ . Then  $\text{rank } E(L) = 2 \text{rank } E(K)$ .*

*Proof.* One way to see this, is to split up  $E(L)$  for the action of  $\text{Gal}(L/K)$ . The twist  $E'/K$  that is associated to the  $-1$ -eigenspace is over  $K$  isogenous

(by an isogeny of degree 3) to  $E$ . Hence  $E(K)$  and  $E'(K)$  have the same rank, and the sum of these two ranks is the rank of  $E(L)$ .

A somewhat different proof runs as follows. Let  $\tau$  denote the non-trivial element of  $\text{Gal}(L/K)$ , and define  $\phi$  on  $E(L)$  by  $\phi(P) = \omega P$ . Consider the sequence

$$0 \rightarrow E(K) \xrightarrow{\phi} E(L) \xrightarrow{\phi^2 + \tau\phi^2} E(K).$$

It is easily verified that this is an exact sequence; e.g., use that  $\phi^2 + \tau\phi^2 = \phi^2 + \phi\tau$  on  $E(L)$ . Moreover, the cokernel of the rightmost arrow is torsion, because  $(1 + \tau)\phi^2\phi^4E(K) = 2E(K)$ . This implies the lemma.  $\square$

Note that this lemma implies for the curve given in theorem 1.1, that although it has rank 18 over  $\mathbb{Q}(t)$ , its rank over  $\mathbb{Q}(t)$  is at most 9. In fact this  $\mathbb{Q}(t)$ -rank is much smaller than 9, as can be calculated using [Br] or alternatively, by computing a characteristic polynomial of Frobenius acting on the second  $\ell$ -adic cohomology group of the elliptic surface over  $\overline{\mathbb{Q}}$  corresponding to  $E$ ; see [vG-T], [Sch, Ch. 2] for details of such a computation.

Combining the two lemmas, one concludes that for any extension  $k(s) = k(t^6) \subset k(t)$  of degree 6 and elliptic curve  $E/k(s)$  given by  $y^2 = x^3 + f(s)$ , one has

$$\text{rank } E(k(t)) = \sum_{n=0}^5 \text{rank } E_n(k(s)),$$

at least if these ranks are finite. As before, here  $E_n$  denotes the elliptic curve given by  $y^2 = x^3 + s^n f(s)$ . In particular this formula holds for all number fields  $k$ , whether or not  $k$  contains a primitive cube root of unity.

### 3. THE RANK 18 EXAMPLE

We will now present a proof of theorem 1.1. In fact, it will be explained at the same time how to construct this example, and even that it is unique in a certain sense.

Consider a polynomial  $f(s) \in \overline{\mathbb{Q}}[s]$  of degree  $d > 0$ , which is not divisible by a 6th power. We assume that  $f(0) \neq 0$ ; this implies that the polynomial  $f(t^6) \in \overline{\mathbb{Q}}[t]$  is 6th power free as well. The elliptic surface over  $\overline{\mathbb{Q}}$  corresponding to the equation  $y^2 = x^3 + f(t^6)$  then has geometric genus  $p_g = d - 1$ . In particular, one obtains a  $K3$ -surface precisely when  $f$  has degree 2. Hence from now on  $E$ , given by the equation  $y^2 = x^3 + at^{12} + bt^6 + c$ , with  $a, b, c \in \overline{\mathbb{Q}}$  satisfying  $ac \neq 0$ , is considered. The elliptic fibration associated with this Weierstrass equation has singular fibres exactly over the roots of  $at^{12} + bt^6 + c = 0$ . If  $b^2 - 4ac = 0$ , then this has 6 zeroes, each with multiplicity 2. This implies that in that case the elliptic  $K3$ -surface has 6 singular fibres, each of Kodaira type  $IV$ . The Shioda-Tate formula then yields the upper bound  $18 - 6 \cdot 2 = 6$  for  $\text{rank } E(\overline{\mathbb{Q}}(t))$ . We will assume that this situation does not occur; in other words,  $b^2 - 4ac \neq 0$ .

By lemma 2.1,  $\text{rank } E(\overline{\mathbb{Q}}(t)) = \sum_{n=0}^5 \text{rank } E_n(\overline{\mathbb{Q}}(s))$ . In the present case,  $E_n$  is given by  $y^2 = x^3 + s^n(as^2 + bs + c)$ . For  $0 \leq n \leq 4$  the corresponding elliptic surface is a rational surface. For such surfaces the Shioda-Tate formula provides an exact formula for  $\text{rank } E_n(\overline{\mathbb{Q}}(s))$  and it is even known that the group is generated by points whose  $x$ -coordinate is a polynomial of degree at most 2. See [Sh90] for details. For  $n = 0, n = 4$  the only reducible

fibre of the associated elliptic surface is of type  $IV^*$ , which implies that the Mordell-Weil rank equals 2. For  $n = 1, n = 3$  one again finds only one reducible fibre; it is of type  $I_0^*$  hence here the rank is 4. In the remaining case  $n = 2$  there are 2 reducible fibres, each of type  $IV$ . This gives 4 as the rank of  $E_2$  over  $\overline{\mathbb{Q}}(s)$ . Adding these contributions and using the proof of lemma 2.1 one now has 16 independent points in  $E(\overline{\mathbb{Q}}(t))$ , all of the form as asserted in the statement of theorem 1.1.

It remains to consider the only eigenspace not taken into account yet, namely the one corresponding to  $E_5$ . The following well known lemma will be used.

**Lemma 3.1.** *Let  $k$  be a field of characteristic 0, and let  $E/k(s)$  be an elliptic curve given by  $y^2 = x^3 + g(s)$ . Suppose that  $g(s) = 0$  has some simple root in an algebraic closure of  $k$ . Then  $E(k(s))$  is a finitely generated free group.*

*Proof.* Since  $g(s)$  has a simple zero,  $E$  is not isomorphic over  $k(s)$  to an elliptic curve already defined over  $k$ . This implies that the Mordell-Weil theorem holds for  $E(k(s))$ ; in other words, it is a finitely generated group. To show that it is torsion free, we specialize at the simple root. This defines a map  $E(\overline{k}(s)) \rightarrow C(\overline{k})$  where  $\overline{k}$  denotes an algebraic closure of  $k$  and  $C$  denotes the curve given by  $y^2z = x^3$  in  $\mathbb{P}^2$ . Since we specialize at a simple root, the singular point on  $C$  is not in the image, and the specialization is in fact a homomorphism of groups. The target group is the additive group  $\overline{k}$ . Hence since such a specialization is known to be injective on torsion points, the lemma follows.  $\square$

Returning to the proof of theorem 1.1, all we have to do in order to have an example of rank 18 is to exhibit a non-trivial point on  $E_5$ , which is the curve given by  $y^2 = x^3 + as^7 + bs^6 + cs^5$ . We will try to find such a point of the simplest possible kind, namely with  $x$ -coordinate a polynomial in  $\overline{\mathbb{Q}}[s]$ . It is clear from the equation that such a polynomial should have degree at least 4. We therefore look at the smallest possible degree, namely 4. The corresponding  $y$ -coordinate should then be a polynomial of degree 6. We can and will assume that the leading coefficients of these coordinates are equal, and then by scaling  $s$  if necessary, that they equal 1. This leads to the problem of finding  $a_0, \dots, a_3$  and  $a, b, c$  and  $b_1, \dots, b_5$  in  $\overline{\mathbb{Q}}$  such that

$$(a_0^3 + b_1s + b_2s^2 + \dots + b_5s^5 + s^6)^2 = (a_0^2 + a_1s + a_2s^2 + a_3s^3 + s^4)^3 + as^7 + bs^6 + cs^5.$$

Using Maple, and eliminating as many as possible of the variables which appear linearly when comparing coefficients, this problem can be solved completely. Apart from solutions with  $a = b = c = 0$ , and multiplying  $a, b, c$  with some given sixth power (which does not change the elliptic curve  $E$ ), one finds the unique additional solution  $(a, b, c) = -27 \cdot (1, -11, -1)$ . The corresponding degree 4 polynomial as  $x$ -coordinate is upto a third root of unity  $x(s) = (s^4 - 12s^3 + 14s^2 + 12s + 1)/4$ . This implies the theorem. Note that in fact  $\text{rank } E_5(\overline{\mathbb{Q}}(s)) = 2$  since it is  $\geq 1$  and even by what we showed above and by the  $\mathbb{Z}[\omega]$ -structure, and it is  $\leq 2$  because of the formula  $\sum \text{rank } E_n(\overline{\mathbb{Q}}(s)) \leq 18$ .  $\square$

*Remark.* It may be of some interest to relate the above construction to the results of Inose and of Kuwata which were mentioned in the introduction.

Start with the  $E_5$  above that has  $\overline{\mathbb{Q}}(s)$ -rank at least 2. This curve corresponds to a  $K3$ -surface over  $\overline{\mathbb{Q}}$ , and the given elliptic fibration on it has precisely 2 reducible fibres, both of type  $II^*$  (at  $s = 0$  and at  $s = \infty$ ). The Shioda-Tate formula for the rank  $\rho$  of the Néron-Severi group of this surface now implies

$$20 \geq \rho \geq 2 + 2 \cdot 8 + \text{rank } E_5(\overline{\mathbb{Q}}(s)) \geq 20,$$

hence we conclude (as before) that  $\text{rank } E_5(\overline{\mathbb{Q}}(s)) = 2$  and also that  $\rho = 20$ .

The result of Inose [In] states, that any  $K3$ -surface which admits a finite rational map to our one, will then also have  $\rho = 20$ . An example of such a surface is the one corresponding to  $E$ ; a rational map in this case is given by  $(x, y, t) \mapsto (x/t^{10}, y/t^{15}, s = t^6)$ . Since the latter surface has no reducible fibres, the Shioda-Tate formula implies that  $\text{rank } E(\overline{\mathbb{Q}}(t)) = 18$  as we already proved.

As a special case of a construction of Kuwata [Ku], take the elliptic curves with equations  $y^2 = x^3 + 1$  and  $y^2 = x^3 - 15x + 22$ . These curves are 2-isogenous, complex multiplication curves. This implies that the Kummer surface of their product is a  $K3$ -surface with a Néron-Severi group of rank 20. An affine equation for this Kummer surface is  $(t^3 + 1)y^2 = x^3 - 15x + 22$ . Now the surface  $X$  corresponding to  $(t^3 + 1)\eta^6 = x^3 - 15x + 22$  admits a rational map of degree 3 to this Kummer surface (given as  $\eta \mapsto y = \eta^3$ ). Note that  $X$  admits an elliptic fibration  $(x, \eta, t) \mapsto \eta$ , with for instance  $\eta \mapsto (x = 2, \eta, t = -1)$  as a section. One computes that a Weierstrass equation for this fibration is  $Y^2 = X^3 + 27 \cdot 16((2\eta^3)^4 + 11(2\eta^3)^2 - 1)$ . Hence the surface  $X$  is over  $\overline{\mathbb{Q}}$  isomorphic to the one presented in theorem 1.1. Note that Inose's result implies that it has Néron-Severi rank 20, hence a third proof for the fact that  $\text{rank } E(\overline{\mathbb{Q}}(t)) = 18$  is obtained. This method of Kuwata has the advantage that it works for other pairs of isogenous CM-curves as well, but only in the present case 18 independent points have been found.

#### 4. OTHER EXAMPLES

Two aspects of the methods above will be discussed: how to apply them in order to find even higher ranks over  $\overline{\mathbb{Q}}(t)$ , and what can be found over  $\mathbb{Q}(t)$ .

**4.1. Higher ranks.** If we are not interested in  $K3$ -surfaces only, it is possible to give examples of the form  $y^2 = x^3 + f(t^6)$  with a higher rank. The following results illustrate this.

**Proposition 4.1.** *Suppose  $f(s) = s^3 + as^2 + as + 1 \in \overline{\mathbb{Q}}[s]$  is a polynomial with simple zeroes. Then  $E/\overline{\mathbb{Q}}(t)$ , given by  $y^2 = x^3 + f(t^6)$  satisfies  $\text{rank } E(\overline{\mathbb{Q}}(t)) \in \{20, 24, 28\}$ . Moreover, there exists  $a \in \overline{\mathbb{Q}}$  for which  $\text{rank } E(\overline{\mathbb{Q}}(t)) \geq 24$ .*

*Proof.* We use lemma 2.1 and the notations introduced there. For a cubic  $f(s)$  as above, the curves  $E_0, E_1, E_2$  and  $E_3$  correspond to rational elliptic surfaces. Adding their contributions yields a subgroup of rank 20 in  $E(\overline{\mathbb{Q}}(t))$ . For the remaining two eigenspaces, note that  $(x, y, s) \mapsto (x/s^4, y/s^6, 1/s)$

defines an isomorphism between  $E_4$  and  $E_5$ . The elliptic  $K3$ -surface corresponding to  $E_4$  has two reducible fibres of type  $IV^*, II^*$  respectively. Hence  $\text{rank } E_4(\overline{\mathbb{Q}}(s)) \leq 18 - 8 - 6 = 4$ . Moreover, we have seen that this rank is even. Since  $\text{rank } E(\overline{\mathbb{Q}}(t)) = 20 + 2 \text{rank } E_4(\overline{\mathbb{Q}}(s))$  this implies the three mentioned possibilities for the rank.

To show that  $\text{rank} \geq 24$  occurs, it suffices by the above and lemma 3.1 to find a value  $a \in \overline{\mathbb{Q}}$  for which  $E_4(\overline{\mathbb{Q}}(s)) \neq \{O\}$ . This can be done as in the proof of theorem 1.1.  $\square$

In fact much higher ranks can be obtained by iterating the method of decomposing the space of sections into eigenspaces. Denote by  $r(f(t))$  the rank of the group  $E(\overline{\mathbb{Q}}(t))$ , where  $E$  is given by  $y^2 = x^3 + f(t)$ . Using this notation, lemma 2.1 gives the formula

$$r(f(t^6)) = r(f(t)) + r(tf(t)) + r(t^2f(t)) + r(t^3f(t)) + r(t^4f(t)) + r(t^5f(t)).$$

If we only use the field automorphism of  $\overline{\mathbb{Q}}(t)$  that multiplies  $t$  by a third or by a second root of unity, the analogous formulas

$$r(f(t^3)) = r(f(t)) + r(t^2f(t)) + r(t^4f(t))$$

and

$$r(f(t^2)) = r(f(t)) + r(t^3f(t))$$

are obtained. Starting with any polynomial  $g(t)$ , the above three formulas can be applied repeatedly until none of the resulting polynomials is a polynomial in  $t^2$  or in  $t^3$ . As an example, one could start with a polynomial  $g$  with  $g(0) \neq 0$  and take  $f(t) = g(t^n)$ . Decomposing as far as possible leads to a certain set of polynomials  $t^a g(t^b)$ , with  $0 \leq a \leq 5$ , and  $\text{gcd}(a, b) = 1$  and  $b$  is a divisor of  $n$  such that  $n/b$  is a power of 2 times a power of 3. This results in a lower bound for  $r(f(t))$  if we take only those contributions  $r(t^a g(t^b))$  that correspond to rational elliptic surfaces. In other words, we only consider the  $a, b$  for which  $a + b \cdot \deg(g) \leq 6$ .

The maximal number of such possible contributions is obtained when one considers  $\deg(g) = 1$ . In this case, in order to have all terms  $r(t^a g(t))$ , we need that  $n$  is a power of 2 times a power of 3 and moreover  $6|n$ . To have the terms  $r(tg(t^2))$  and  $r(t^3g(t^2))$  as well leads to the additional assumption  $12|n$ . Next, the terms  $r(tg(t^3))$  and  $r(t^2g(t^3))$  are present if also  $18|n$ . And finally the term  $r(tg(t^4))$  appears in addition by demanding  $24|n$ . The result one obtains in this way, is the following.

**Proposition 4.2.** *Let  $n$  be a positive multiple of 72 and let  $g(t) \in \overline{\mathbb{Q}}[t]$  be a degree 1 polynomial with  $g(0) \neq 0$ .*

*The curve given by  $y^2 = x^3 + g(t^n)$  has rank  $\geq 36$  over  $\overline{\mathbb{Q}}(t)$ . Moreover, one can find 36 independent points all coming from rational elliptic surfaces via a base change.*

*If  $n$  is a positive multiple of 360, then the rank of this curve over  $\overline{\mathbb{Q}}(t)$  equals 68. Here 60 independent points come from rational elliptic surfaces via a base change, and 8 more in the same way from an elliptic  $K3$ -surface.*

*Proof.* As already remarked in the introduction of this paper, the rank 68 example here is due to Shioda. Using his algorithm [Sh86, Thm. 1], one can in particular calculate the rank of any curve as given in the proposition; the result is that the rank is  $\leq 68$ , with equality if and only if  $n$  is a positive

multiple of 360. We will now follow the discussion above. This will lead to 36 resp. 60 independent points coming from the various associated rational elliptic surfaces. Note that in particular, such points may be explicitly given.

To prove the first part of the proposition, note that  $r(g(t^n)) \geq r(g(t^m))$  if  $m|n$ . Hence we may and will assume  $n = 72$ . Then

$$\begin{aligned} r(g(t^72)) &\geq r(g(t^6)) + r(tg(t^2)) + r(t^3g(t^2)) + r(tg(t^3)) + r(t^2g(t^3)) + r(tg(t^4)) \\ &= 8 + 4 + 4 + 6 + 6 + 8 = 36, \end{aligned}$$

which is what we wanted to prove.

It remains to prove the assertions about the case of a positive  $n \equiv 0 \pmod{360}$ . In the discussion preceding proposition 4.2, we only considered rational eigenspaces corresponding to  $g(t^6)$ ,  $tg(t^4)$ ,  $tg(t^3)$ ,  $t^2g(t^3)$  and  $tg(t^2)$ ,  $t^3g(t^2)$ . One can use the remaining ones, for  $g(t^5)$  and  $tg(t^5)$  as well, by relaxing the assumption that some eigenspace corresponds to  $y^2 = x^3 + t^a g(t^b)$  to the weaker statement that the points on such a curve give rise to a subspace (of possibly smaller dimension) in an eigenspace. We illustrate this by an example. Starting from the polynomial  $g(t^{30})$ , one of the eigenspaces when using the automorphism of order 6 will correspond to  $t^5g(t^5)$ . Using our automorphisms of order 2, 3 or 6, we cannot decompose this space into smaller pieces. However, the invariants for the order 5 automorphism that multiplies  $t$  by a fifth root of unity, will give a subspace corresponding to  $sg(s)$ . Hence  $r(t^5g(t^5)) \geq r(tg(t))$ , and the latter number may correspond to a rational surface even though the first one does not. Although it will not be used here, we remark that such a difference  $r(t^5g(t^5)) - r(tg(t))$  is a multiple of 8. To prove this, note that we consider the  $\mathbb{Q}(\omega)$ -vector space  $V = E(\overline{\mathbb{Q}}(t)) \otimes_{\mathbb{Z}} \mathbb{Q}$  here, with  $E$  given by  $y^2 = x^3 + t^5g(t^5)$ . This vector space comes equipped with an action of a cyclic group of order 5. Since a nontrivial fifth root of unity generates an extension of degree 4 over  $\mathbb{Q}(\omega)$ , the representation on  $V$  splits into a sum  $V_{\text{tr}} \oplus V_{\text{nt}}$ , where the action on  $V_{\text{tr}}$  is the trivial one and where  $V_{\text{nt}}$  is a sum of 4-dimensional irreducible representations. In particular,  $\dim_{\mathbb{Q}(\omega)} V_{\text{nt}}$  is a multiple of 4, and therefore  $r(t^5g(t^5)) - r(tg(t)) = \dim_{\mathbb{Q}} V_{\text{nt}}$  is a multiple of 8.

We now discuss a number of eigenspaces that come up when starting with a polynomial  $g(t^{360})$ . Here  $g$  is a polynomial of degree 1. Throughout, the assumption  $g(0) \neq 0$  is made. Only in the spaces associated with  $g(t^{60})$ ,  $t^2g(t^{60})$ ,  $t^3g(t^{60})$  and  $t^4g(t^{60})$  we are able to find pieces corresponding to rational elliptic surfaces.

$t^2g(t^{60})$ . Using order 2 automorphisms, this part yields

$$\begin{aligned} r(tg(t^{30})) + r(t^4g(t^{30})) &\geq r(t^2g(t^{15})) + r(t^5g(t^{15})) \\ &\geq r(tg(t^3)) = 6. \end{aligned}$$

$t^4g(t^{60})$ . Analogous to the previous part, one finds here

$$\begin{aligned} r(t^2g(t^{30})) + r(t^5g(t^{30})) &\geq r(tg(t^{15})) + r(t^4g(t^{15})) \\ &\geq r(t^4g(t^{15})) = r(t^6 \cdot t^4g(t^{15})) \\ &\geq r(t^2g(t^3)) = 6. \end{aligned}$$

$t^3g(t^{60})$ . Here a splitting into three parts can be used; it gives

$$\begin{aligned} r(tg(t^{20})) + r(t^3g(t^{20})) + r(t^5g(t^{20})) &\geq r(t^5g(t^{20})) \\ &\geq r(tg(t^4)) = 8. \end{aligned}$$

$g(t^{60})$ . In this case one obtains a splitting into 6 parts, corresponding to the polynomials  $t^n g(t^{10})$  for  $0 \leq n \leq 5$ . These parts will now be analyzed separately.

$n = 5$ . We estimate  $r(t^5 g(t^{10})) \geq r(tg(t^2)) = 4$ .

$n = 4$ . Analogously,  $r(t^4 g(t^{10})) = r(t^{10} g(t^{10})) \geq r(t^2 g(t^2)) = 4$ .

$n = 3$ . This gives  $r(t^3 g(t^{10})) = r(t^{15} g(t^{10})) \geq r(t^3 g(t^2)) = 4$ .

$n = 2$ . Using a further splitting one obtains

$$\begin{aligned} r(t^2 g(t^{10})) &= r(tg(t^5)) + r(t^4 g(t^5)) \\ &= r(tg(t^5)) + r(t^{10} g(t^5)) \\ &\geq r(tg(t^5)) + r(t^2 g(t)) = 8 + 2 = 10. \end{aligned}$$

$n = 0$ . Just as in the previous case,

$$\begin{aligned} r(g(t^{10})) &= r(g(t^5)) + r(t^3 g(t^5)) \\ &= r(g(t^5)) + r(t^{15} g(t^5)) \\ &\geq r(g(t^5)) + r(t^3 g(t)) = 8 + 2 = 10. \end{aligned}$$

$n = 1$ . This last part cannot be split into more manageable pieces using automorphisms that multiply  $t$  by a root of unity. However, it is possible to use the fact that in the surface corresponding to  $y^2 = x^3 + tg(t^{10})$ , the fibres over 0 and over  $\infty$  are the same. To obtain somewhat simpler formulas, note that after scaling  $x, y, t$  by some non-zero elements of  $\overline{\mathbb{Q}}$  one can assume  $g(s) = s + 1$ ; we will do this here. An alternative equation for the one above (replace  $x, y$  by  $x/t^2, y/t^3$ , respectively) is now  $y^2 = x^3 + t^5 + 1/t^5$ . This is clearly invariant under  $t \mapsto 1/t$ . Hence with  $u = t + 1/t$ , we have a quadratic extension  $\overline{\mathbb{Q}}(t)/\overline{\mathbb{Q}}(u)$  and a curve  $E/\overline{\mathbb{Q}}(u)$ , for which we are interested in the points over the quadratic extension. As before, these points can be split (up to groups of finite index) into  $E(\overline{\mathbb{Q}}(u))$  and  $E'(\overline{\mathbb{Q}}(u))$ . Here  $E'$  is the corresponding quadratic twist.

Since  $t^5 + 1/t^5 = u^5 - 5u^3 + 5u$ , one finds that  $E(\overline{\mathbb{Q}}(u))$  corresponds to the sections of a rational elliptic surface without reducible fibres. In particular it has rank 8. The quadratic extension  $\overline{\mathbb{Q}}(t)/\overline{\mathbb{Q}}(u)$  is obtained by adjoining a square root of  $u^2 - 4$ . Hence one concludes

$$r(tg(t^{10})) = r(t^5 - 5t^3 + 5t) + r((t^2 - 4)^3(t^5 - 5t^3 + 5t)) \geq 8.$$

Summing all lower bounds described above, one finds 60 independent points on Shioda's example, and all these points can be interpreted in terms of rational elliptic surfaces.

It remains to prove the assertion about the remaining rank  $68 - 60 = 8$  part. One can of course use Shioda's algorithm from [Sh86, Thm. 1] to find all other contributions  $r(t^a g(t^b))$ . This results in the equality  $r(tg(t^{10})) = 16$ . Since we only used the lower bound 8, this is where the remaining sections may be found.

Alternatively, this is seen as follows. Start with the  $K3$ -surface  $Y$  corresponding to  $y^2 = x^3 + s^5 g(s^2)$ . Since the elliptic fibration coming from this equation has 2 fibres of type  $II^*$ , the Néron-Severi rank  $\rho(Y)$  of  $Y$  is at least  $2 + 2 \cdot 8 = 18$ . Substituting  $s = t^6, x = t^8 \xi, y = t^{12} \eta$  yields a finite rational map  $X \rightarrow Y$ , with  $X$  the  $K3$ -surface corresponding to  $\eta^2 = \xi^3 + tg(t^{10})$ . In particular, using Inose's result from [In] once more,

one concludes  $\rho(X) = \rho(Y) \geq 18$ . Since the obvious elliptic fibration on  $X$  contains no reducible fibres, this implies  $r(tg(t^{10})) \geq 16$ . Using

$$\begin{aligned} r(tg(t^{10})) &= r(t^5 - 5t^3 + 5t) + r((t^2 - 4)^3(t^5 - 5t^3 + 5t)) \\ &= 8 + r((t^2 - 4)^3(t^5 - 5t^3 + 5t)) \end{aligned}$$

as was shown above, one finds that the remaining 8 sections are in fact on the elliptic  $K3$ -surface with equation  $(t^2 - 4)y^2 = x^3 + t^5 - 5t^3 + 5t$ . This finishes the proof of proposition 4.2.  $\square$

*Remark 1.* It may be interesting to note that in [Fa], Fastenberg proved that under some conditions which do not hold in our examples, an elliptic curve  $E/\mathbb{C}(t)$  has finite rank over the union of all extensions  $\mathbb{C}(t^{1/n})$ . Shioda's upper bound 68 given in proposition 4.2 shows that this is also true for the curve given by  $y^2 = x^3 + at + b$ , provided that  $ab \neq 0$ .

*Remark 2.* Many variations on these ideas are possible. For instance, starting from a quadratic polynomial  $f(t)$  such that  $r(f(t^6)) = 18$  (theorem 1.1 shows an example), one can use Inose's result to conclude that  $r(tf(t^5)) = 18$  as well, and  $r(t^3f(t^2)) = r(t^5f(t^2)) = 6$ . Combining as before, one finds  $r(f(t^{60})) \geq 54$ , where all these points come from rational or from  $K3$ -surfaces.

**4.2. Ranks over the rational numbers.** If one restricts to curves  $E/\mathbb{Q}(t)$ , lemma 2.2 implies that the possible rank here is at most half the rank over  $\overline{\mathbb{Q}}(t)$ . However, it seems quite hard to get anywhere near such a bound. Mestre [Me] published an example of a  $j = 0$ -curve which cannot be defined over  $\mathbb{Q}$  and which has 7 independent points over  $\mathbb{Q}(t)$ . His curve is not of the form  $y^2 = x^3 + f(t^6)$  as is studied here. We tried to find some high rank examples of this form, by demanding that various associated eigenspaces contain  $\mathbb{Q}(t)$ -rational points. The description by Bremner [Br] of certain classes of curves with positive  $\mathbb{Q}(t)$ -rank is useful here. Nevertheless, we had very limited success.

The curve given by  $y^2 = x^3 + t^{12} - 26t^6 - 343$  contains 4 independent points over  $\mathbb{Q}(t)$ , namely with  $x$ -coordinates 8,  $(-t^6 + 49)/t^2$ ,  $t^6 + 7$  and  $(9t^{12} + 86t^6 + 49)/(16t^2)$ . This curve is birational to the one with equation  $F(X, Y) = 1$ , for

$$F(X, Y) = Y^3 + (X - Y)(X - 2Y)(X - (1 - t^3)Y/2).$$

In terms of the latter equation, we consider rational points with  $Y = 0, 1$  or with  $X = 0$ .

The curve with equation  $y^2 = x^3 + t^{18} + 2973t^{12} + 369249t^6 + 11764900$  contains 5 independent  $\mathbb{Q}(t)$ -rational points. This example already appeared in [S-T], where it was explained how it is obtained by the same construction that Mestre used when he finds his rank  $\geq 7$  example.

## REFERENCES

- [Br] A. Bremner, *Some simple elliptic surfaces of genus zero*, Manuscr. Math., **73** (1991), 5–37.
- [Co] D.A. Cox, *Mordell-Weil groups of elliptic curves over  $\mathbb{C}(t)$  with  $p_g = 0$  or 1*, Duke Math. J., **49** (1982), 677–689.
- [Fa] L.A. Fastenberg, *Mordell-Weil groups in procyclic extensions of a function field*, Duke Math. J., **89** (1997), 217–224.

- [vG-T] B. van Geemen and J. Top, *Selfdual and non-selfdual 3-dimensional Galois representations*, Compos. Math., **97** (1995), 51–70.
- [In] H. Inose, *On certain Kummer surfaces which can be realized as non-singular quartic surfaces in  $\mathbb{P}^3$* , J. Fac. Sci. univ. Tokyo, **23** (1976), 545–560.
- [Ku] M. Kuwata, *Elliptic K3 surfaces with high Mordell-Weil rank*, preprint, 1996.
- [Me] J-F. Mestre, *Rang de courbes elliptiques d'invariant nul*, C.R. Acad. Sci. Paris, Sér. I, **321** (1995), 1235–1236.
- [Ni] K.I. Nishiyama, *Examples of Jacobian fibrations on some K3 surfaces whose Mordell-Weil lattices have the maximal rank 18*, Comm. Math. univ. St. Pauli, **44** (1995), 219–223.
- [Sch] J. Scholten, *Mordell-Weil groups of elliptic surfaces and Galois representations*, PhD thesis, Groningen, 2000.
- [Sh72] T. Shioda, *On elliptic modular surfaces*, J. Math. Soc. Japan, **24** (1972), 20–59.
- [Sh86] T. Shioda, *An explicit algorithm for computing the Picard number of certain algebraic surfaces*, Am. J. of Math., **108** (1986), 415–432.
- [Sh90] T. Shioda, *On the Mordell-Weil lattices*, Comm. Math. univ. St. Pauli, **39** (1990), 211–240.
- [Sh92] T. Shioda, *Some remarks on elliptic curves over function fields*, Astérisque, **209** (1992), 99–114.
- [Sil] J.H. Silverman, *The arithmetic of elliptic curves*. Springer-Verlag, New York etc., GTM 106, 1986/1992.
- [S-T] C.L. Stewart and J. Top, *On ranks of twists of elliptic curves and power-free values of binary forms*, Journ. AMS, **8** (1995), 943–973.

DEPARTMENT OF MATHEMATICS, BRIGHAM YOUNG UNIVERSITY, PROVO, UT 84602-6539, USA

*E-mail address:* `jasbir@math.byu.edu`

VAKGROEP WISKUNDE RuG, P.O. Box 800, 9700 AV GRONINGEN, THE NETHERLANDS

*E-mail address:* `top@math.rug.nl`